GNT Inscription Connexion

# Piratage de distributeurs : des billets en libre-service ?

Le dimanche 15 Juin 2014 à 12:10 par Jérôme G.

**L'avis d'expert de Kirill Kruglov, chercheur chez Kaspersky Lab, après la médiatisation du piratage d'un distributeur automatique de billets par deux enfants au Canada.**

Est-ce étonnant que deux enfants canadiens aient pu pirater un distributeur automatique de billets à l'aide d'un manuel trouvé sur Internet ? Nous aimerions penser que oui et pourtant **cette affaire n'est que l'illustration d'une réalité toute simple : les distributeurs automatiques sont des appareils informatiques comme les autres**. S'ils ne sont pas protégés par un mot de passe fort et renforcés avec des équipements interdisant l'accès aux ressources de gestion à des tiers ( ce qui n'a apparemment pas été le cas au Canada ), ils peuvent être aussi vulnérables qu'un ordinateur familial.

L'utilisateur du mot de passe par défaut tel qu'il est donné dans le manuel d'utilisation est une énorme faille de sécurité. Il n'est même pas question ici des limites d'un logiciel, mais de l'absence complète de sécurité Informatique.

Cependant, ce que ces deux enfants ont réussi à faire n'est que l'une des nombreuses façons de pirater un distributeur de billets car **il existe bien d'autres façons pour des criminels de pénétrer dans le système, même s'il est protégé**. Deux sont particulièrement inquiétantes : les attaques réseaux et celles utilisant des équipements amovibles.

Les attaques faisant appel à des équipements amovibles ne sont pas courantes, en partie car les réseaux bancaires sont le plus souvent bien protégés. Les attaques réseau visent plutôt les terminaux de points de vente et caisses enregistreuses informatisées, qui sont le plus souvent connectés à des réseaux traditionnels plus vulnérables au cyberattaques.

Une attaque de DAB classique peut se faire en deux étapes seulement. Tout d'abord, les criminels vont télécharger un petit logiciel ( malware, exploit, etc. ) sur un appareil amovible USB ou un CD. Après avoir réussi à connecter l'appareil USB au DAB, le logiciel va permettre aux utilisateurs de bénéficier des droits d'administration à un haut niveau et ainsi pouvoir lancer le malware. Les criminels peuvent également choisir une autre approche, à savoir initialiser un DAB depuis un CD. En désactivant les polices et les logiciels de sécurité en place dans la machine, il ne leur reste plus qu'à déposer le malware directement sur le disque dur. Il est ensuite exécuté par l'OS. Cela pourrait prendre la forme d'un backdoor contrôlant l'OS du DAB par exemple. Une fois que le distributeur a été hacké, il ne reste plus aux criminels qu'à récupérer les billets qui s'y trouvent.

En ce qui concerne les terminaux de points de vente, la technique utilisée est un peu différente. Les criminels installent un composant malicieux qui leur permet de lire la mémoire RAM du terminal. Ce composant va ensuite récupérer les informations liées aux cartes utilisées pour les transactions enregistrées. Une fois l'opération terminée, le malware se connecte de nouveau au serveur du centre de commandes et de contrôle mis en place par les criminels et y transfère les données.

**Rien de ce que je viens de décrire n'est nouveau, pourtant ces techniques sont toujours utilisées avec succès comme peut en attester le groupe américain Target qui en a été victime l'automne dernier.**

Pour se protéger de tels incidents, les banques et les entreprises de commerce doivent déployer une combinaison d'outils de protection. Dans

certains cas, une simple combinaison pare-feu / antivirus suffit, dans d'autres il faut des équipements spécialisés. En ce qui concerne les distributeurs automatiques de billets, particulièrement exposés et sensibles, nous recommandons un arsenal d'armes sophistiquées, à l'image de l'encryption, le contrôle des appareils mobiles, un système de prévention des intrusions réseau, une technologie de prévention des exploits et une solution de contrôle des applications en mode default deny.

**Complément d'information**

**Insolite : deux enfants de 14 ans piratent un distributeur de billets de banque**

**Meilleures vidéos de la semaine : distributeur Free Mobile, Galaxy S5, Star Citizen, Oculus Rift**

Voir les 4 commentaires

J'aime Tweet g+ +1

## Vos commentaires

DeepBlueOcean

6715 points

Le groupe américain "Target" ....
Si bien nommé pour les attaques ....
La cible des criminels, et quand ça fait mouche ... ça banque

Répondre en citant

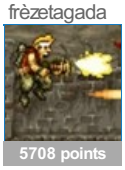
bugmenot

2849 points

Bon, c'est pas tout ça, mais quand est-ce qu'on passe aux travaux pratiques?

Répondre en citant

frèzetagada



5708 points

Pour obtenir des infos sur la triche ou des super-pouvoirs normalement non disponibles, pour les jeux vidéo, il y a gameFAQs.com .

Pour les DAB, c'est quoi le site ?!?

Répondre en citant

Du974

Pour les DAB c'est saint-laurent-du-maroni.com

900 points
Premium

Répondre en citant

## Poster un commentaire

Anonyme

Poster le commentaire

A propos Contacts Publicité Partenaires Conditions d'utilisation
Signaler un bug
Copyright © 2001-2014 GNT Media, tous droits réservés